discussing various instruments that could apply to deployment, such as incentives to road operators or cities.[195]

b) Comparison of United States to Asia

In Asia, Japan and Korea are most active in DSRC development, with Japan leading. In both countries, the initial focus is on adapting the Electronic Toll Collection system operating at 5.8 GHz. The Japanese government has deployed 5.8 GHz "ITS Spots," which communicate with electronic toll tags to offer limited V2X safety capabilities, as well as mobility and convenience services. Additionally, some Japanese automotive OEMs (mainly Toyota) are actively supporting the deployment of V2X using 760 MHz communications. Japan appears likely to proceed with a two-band solution, and suppliers have prototyped transceivers covering both bands. Deployment of 760 MHz systems could come as soon as 2014.

In China, this band is reserved for potential ITS use as well. There have been indications that Korea seeks to shift to 5.9 GHz to be more compatible internationally, but no announcements have been made. No information was discovered indicating any interest from China for ITS applications in the 5.9 GHz band.

Development of message sets in Japan is not yet complete but appears to be toward the BSM/CAM[196]/DENM[197] message sets. Harmonization of probe data message sets is currently underway between Japan and the U.S. Similar to the approach in Europe, deployment in Japan is mostly market-driven, with the government leading to provide initial roadside capability in the case of the 5.8 GHz system, and some OEMs pushing for the 760 MHz system for V2V crash avoidance.

The Japanese 5.8 GHz system is not compatible with the IEEE 802.11p protocol used in the U.S. and Europe, due to a Japanese law requiring legacy protocols. At the security level, there are advocates of using IEEE 1609.2 as the security framework, which would be compatible with the U.S. and Europe, but this has not yet been decided.

[195] *Id.*, at 39.
[196] Cooperative Awareness Message.
[197] Decentralized Environmental Notification Message.

VI. V2V Safety Applications

NHTSA reviewed the existing information on various safety applications that leverage V2V communications and on various driver-vehicle interface options. NHTSA's goal in this effort was to determine:

- The extent to which the available performance and test metrics cover the variety of circumstances under which crashes occur that V2V-based safety applications could address; and
- Whether the metrics are practicable, repeatable, objective, and can clearly distinguish systems that pass from those that fail.

A. Performance metrics currently available for V2V safety applications

There are a number of performance and test metrics currently available that can be used to evaluate the performance of the research-stage prototype V2V safety applications and systems. This information can provide a useful foundation for the agency to consider and build upon to potentially establish Federal Motor Vehicle Safety Standards.

While the existing performance and test metrics cover the main conditions under which each of these crash types occur, a common theme among the performance metrics for all of the applications is the lack of testing under all conditions within the context of the safety problem, including, for example, poor weather or road conditions. To move forward with regulatory action to mandate safety applications, the agency would need to understand whether performance and test metrics can take into account these less-than-ideal conditions. As an example, the safety problem contains crashes that occur on wet pavement, which increases vehicle stopping distances, requiring adjustments to when advisories or warnings would be provided to a driver: advisories or warnings should be provided sooner if more time is needed for the driver to respond or for the vehicle to perform. However, this would need to be balanced with the potential for advisories or warnings to become nuisances to the driver, which could reduce system benefit.

With this in mind, the agency will need to evaluate crash statistics further to better understand what percentage of crashes happen under less-than-ideal conditions and how potential adjustment to warning activation may help drivers. Current crash data indicates that *most* crashes happen under ideal conditions, but further analysis may yield opportunities that could be addressed by V2V technology. This research would also focus on providing clear rationales for the inclusion or exclusion of any performance and test metrics.

In addition to considering how the existing performance and test metrics could be refined, further development will help ensure the metrics are practicable, repeatable, and can clearly distinguish systems that conform to the performance metrics from those that do not.

B. The safety applications

This section focuses on the following V2V safety applications that address common rear-end, opposite direction, junction crossing, and lane change crash scenarios, as shown in Table VI-1 and described below:

Table VI-1 V2V Safety Applications

Crash Type	Safety Application
Rear-End	Forward Collision Warning (FCW)
	Electronic Emergency Brake Light
Opposite direction	Do Not Pass Warning
	Left Turn Assist (LTA)
Junction crossing	Intersection Movement Assist (IMA)
Lane change	Blind Spot Warning + Lane Change Warning (BSW+LCW)

- FCW: Warns the driver of an impending rear-end collision with another vehicle ahead in traffic in the same lane and direction of travel.
- EEBL: Warns the driver of another vehicle that is braking hard farther up ahead in the flow of traffic. The braking vehicle does not necessarily have to be in the direct line of sight of the following vehicle, and can be separated by other vehicles.
- DNPW: Warns the driver of one vehicle during a passing maneuver attempt when a slower-moving vehicle, ahead and in the same lane, cannot be safely passed using a passing zone that is occupied by vehicles in the opposite direction of travel. The application may also provide the driver an advisory warning that the passing zone is occupied when a passing maneuver is not being attempted.
- LTA: Warns the driver of a vehicle, which is beginning to turn left in front of a vehicle traveling in the opposite direction, that making a left turn, at this time, would result in a crash.
- IMA: Warns the driver when it is not safe to enter an intersection due to high collision probability with other vehicles at controlled (with stoplights) and uncontrolled (with stop, yield, or no signage) intersections.
- BSW + LCW: Warns the driver during a lane change attempt if the blind spot zone into which the driver intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. The application also provides the driver with advisory

information that another vehicle in an adjacent lane is positioned in the original vehicle's "blind spot" zone when a lane change is not being attempted.

C. Key Findings for each V2V Safety Application

1. Forward Collision Warning

Forward Collision Warning is an application that currently has well-developed research-level performance and test metrics. The agency's analysis identified where more information would be needed to fully explore the issues that could arise in a regulatory action regarding V2V safety applications, such as a supporting rationale that clearly explains the safety risk/crash scenario that each metric is designed to address and how the metric will address that risk/scenario. Test metrics have been developed by CAMP and have been further refined by Volpe in support of the Track 4A Forward Collision Avoidance project. Test metrics for non-V2V forward collision systems were also developed for NHTSA's New Car Assessment Program (NCAP) and the In-Vehicle Based Safety Systems (IVBSS) project. Many of these performance and test measures may be applicable to a V2V-based FCW application; however, additional metrics will need to be developed based on V2V's unique capabilities, such as the DSRC radio operating in inclement weather and being able to detect vehicles beyond the current capabilities of radar and visual sensors.

The test procedures for FCW developed by CAMP and Volpe address all three of the priority pre-crash scenarios included in the rear-end crash group: Lead Vehicle Stopped, Lead Vehicle Decelerating, and Lead Vehicle Moving. These three scenarios comprise 93 percent of the rear-end crashes. Additionally, several of the test scenarios developed address variations of the striking maneuver crash scenario, which, while comprising a small number of rear-end crashes, represents an incremental benefit that can be gained by a V2V-based FCW system. While not explicitly tested, the FCW application also has the potential to address the additional two Lead Vehicle Accelerating scenarios, which comprise the other 7 percent of the rear-end crash group

However, additional analysis is necessary to ensure that each performance and test metric is sufficiently supported by a clear rationale. The specifics of these test procedures, such as their required alert timing, speeds at which the test is run, and radius of curvature, vary in detail across the developing organizations, and the agency believes they may need to be further refined to better reflect the safety problem.

2. Emergency Electronic Brake Lights

Emergency Electronic Brake Light addresses_the Lead Vehicle Decelerating scenario and shares some overlap in functionality with the Forward Collision Warning application. EEBL issues a warning to the driver when the lead vehicle is decelerating by a minimum of 0.4 g. Previous research indicated that relatively severe braking (0.55 g or higher) by the lead vehicle in LVD crashes accounts for approximately 15 percent of the total number of LVD crashes.[198]

3. Do Not Pass Warning

The agency found that the Do Not Pass Warning application currently has a less robust set of performance and test metrics compared to other V2V safety applications studied. Do Not Pass Warning addresses only a subset of opposite direction crashes because it addresses situations where the driver is intentionally conducting a passing maneuver using the lane of opposing traffic. The safety data indicate that the vast majority (approximately 90 percent) of opposite direction crashes occur when a driver unintentionally drifts into a lane with oncoming traffic (as opposed to drivers conducting a passing maneuver). The current design of the DNPW application, however, issues a warning to the driver only when the driver activates his turn signal when changing lanes.

The current test metrics that are available also do not test the DNPW application's ability to function under a wide variety of roadway conditions (e.g., under various road curvatures which may exceed the capabilities of the path prediction algorithm). For example, as 25 percent of the opposite direction crashes resulting from a passing maneuver do occur under varying roadway conditions, the currently-available test metrics may need to be altered or supplemented in order to test for those conditions.

4. Left Turn Assist (LTA)

Left Turn Assist is an application that addresses left turn across path/opposite direction crashes that constitutes approximately 7.4 percent of all light vehicle crashes. Recent research suggests that while executing a turn, drivers activate the turn signal about 75 percent of the time.[199] Current performance and test metrics for LTA require turn signal activation to activate the safety application. Although the research has suggested potential methods to predict left turns without an active turn signal, either (1) the application will need more development to predict

[197] Analyses of Rear-End Crashes and Near-Crashes in the 100-Car Naturalistic Driving Study to Support Rear-Signaling Countermeasure Development (Lee, Llaneras, Klauer, & Sudweeks, 2007, Report No. DOT HS 810 846). See www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2007/Analyses%20of%20Rear-End%20Crashes%20and%20Near-Crashes%20(DOT%20HS%20810%20846).pdf (last accessed Mar. 4, 2014).

[199] Turn Signal Usage Rate Results: A Comprehensive Field Study of 12,000 Observed Turning Vehicles (Ponziani, 2012, SAE Technical Paper 2012-01-0261). See http://papers.sae.org/2012-01-0261/ (last accessed Jan. 29, 2014).

left turns without a signal or (2) this information should be used to discount the estimated safety benefits of this application when turn signal activation is the only indication of driver intent.

However, there is some risk that relying on driver intent may produce false warnings resulting from the ambiguities of determining driver intent to execute a left turn. Finally, more testing would be required to ensure the values are tuned to the optimal values to determine when to provide imminent or advisory warnings compared to the current metrics. Further testing and tuning may potentially minimize false warnings. The OEMs understand that the current configuration of LTA that requires turn signal activation to indicate driver intent limits the application's effectiveness. As indicated above, the OEMs agree that more development is needed to ascertain driver intent not only for LTA but for other crash avoidance applications. However, various OEMs have indicated that this work is OEM-specific and each will investigate other methods to ascertain driver intent to support their individual safety applications.

5. Intersection Movement Assist (IMA)

Intersection Movement Assist has the potential for significant safety benefits and cost savings. As designed, IMA should address five types of junction-crossing crashes. These crashes, which collectively represent 26 percent of all crashes occurring in the crash population and 23 percent of comprehensive costs, can be categorized as follows: straight crossing paths at non-signal, left turn into path at non-signal (LTIP), right turn into path at signal (RTIP), running red light, and running stop sign.

Initial Safety Pilot Model Deployment results indicated there is opportunity for this application to issue false warnings in a real-world environment. Various roadway geometries (e.g., cloverleaf, on-ramp, exit ramp) that do not represent a crash-imminent situation can be incorrectly classified as conflict situations by the system. Improvements to the IMA algorithm for the second stage of driver evaluations indicate these false warnings can be improved as the algorithms mature through additional testing. It may be necessary to develop new performance and test metrics that are designed to mitigate false warnings on different roadways such as curved roads and at non-perpendicular intersections.

6. Blind Spot +Lane Change Warning

Blind Spot Warning/Lane Change Warning is an application that provides an advisory alert when another vehicle occupies the adjacent lane in the driver's blind spot. This advisory elevates to a warning when the driver signals his intent to change lanes through the activation of the turn signal. An advisory is not elevated to a warning if a driver unintentionally drifts into an adjacent lane, i.e., does not indicate intent by activating a turn signal. Additionally, drivers infrequently use turn signals in lane change near-crash events (<26 percent turn signal use, based upon an unpublished analysis of IVBSS data).[200] As a result, the application has the potential to address at least 19 percent of the crashes in the lane change crash group.[201]

D. Key conclusions for each application

1. Forward Collision Warning

Current FCW applications based on visual and radar detection systems can be stymied by certain lighting and weather conditions, and are limited with respect to distance. FCW applications using V2V technology can function in environments and under conditions beyond the current visual and radar detection systems (e.g., sunrise, sunset, rain, snow, >300m range), allowing for a more robust warning system. Some further refinement of performance and test metrics is advisable to align V2V-based FCW applications better to the safety problem, and to more clearly specify each of those metrics with a supporting rationale. With further development of the performance and test metrics, potentially greater safety benefits can be realized with a V2V FCW application, or a combined V2V and sensor-based system, as compared to visual or radar-based systems without V2V.

2. Blind Spot Warning + Lane Change Warning

BSW/LCW is an application that provides an advisory alert when another vehicle occupies the adjacent lane in the driver's blind spot. This advisory elevates to a warning (LCW) when the driver signals his intent to change lanes through the activation of the turn signal.

As discussed, lane change maneuvers can be either purposeful or accidental, and they may or may not involve use of the turn signal. In order to cover the variety of potential crash situations, it is recommended that other indicators of driver intent and vehicle movement be identified in addition to the turn signal, as well as ways of measuring them for use in a LCW application. Finally, the test metrics established to evaluate these systems need to test the LCW when vehicles are traveling at varying speeds between the host vehicle and remote vehicle to align more closely with the safety need.

3. Do Not Pass Warning

Do Not Pass Warning has the potential to reduce crashes that are not easily addressed by the limited detection range and line of sight capabilities of radar or camera systems. Incremental safety benefits can be realized from Do Not Pass Warning alone; however, as currently designed

[200] Data provided by Dr. W. Najm in 5/3/13 email, based upon analysis of IVBSS data. See Docket No. NHTSA-2014-0022

[201] Depiction of priority light-vehicle pre-crash scenarios for safety applications based on vehicle-to-vehicle communications (Najm, Toma, and Brewer, 2013, Report No. DOT HS 811 732). See: www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print (last accessed Jan. 29, 2014).

with reliance on turn signal activation and with functional limitations under certain road conditions (e.g., road curvatures), the application's benefits may not be as large as those from other applications. As an addition to a suite of other V2V safety applications, DNPW may be useful for realizing safety benefits at little marginal cost.

However, when only considering this smaller portion of opposite direction crashes the DNPW application has the potential to be well-suited for addressing this crash problem because V2V communications afford vehicles a rich set of information (e.g., position and trajectory) regarding the other vehicles on the road over a long distance.

DNPW could offer improved range over sensor-based systems and it may be advisable to investigate fused V2V and sensors systems and their ability to address DNPW-related crash situations.

4. Left Turn Assist

Left Turn Assist addresses the majority of crashes at intersections in which the turning vehicle is using the left turn signal. As stated above, research suggests that approximately 75 percent of drivers use turn signals when executing turns. Although previous research[202] efforts have suggested potential methods to predict left turns without an active left turn signal, either (1) the application will need more development to develop prediction techniques or (2) the benefits for this application must be discounted when turn signal activation is the only indication of driver intent.

It may be advisable for LTA to also consider yaw rate and steering wheel angle along with turn signal activation, heading, and vehicle speed to help determine driver intent and whether to issue a warning. However, these additions could affect the implementation of aftermarket safety devices.

Overall, a driver's failing to activate turn signals when making left turns is the largest limiting factor to the effectiveness of this application, reducing the number of crashes this application could potentially address by 1.9 percent. The proper formulation of performance metrics needs to consider all real-world driving situations that can be addressed by the LTA application. If performance metrics cannot address certain real-world conditions, we may not be

[202] The Time Course of a Lane Change: Driver Control and Eye Movement Behavior (Salvucci and Liu, 2002, Transportation Research, Part F, 5(2): 123-132). See http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.2172&rep=rep1&type=pdf (last accessed Jan. 29, 2014); also See Modeling Differences in Behavior Within and Between Drivers (Liu, 2011) in Human Modeling in Assisted Transportation: Models, Tools and Risk Methods, in 15-22 (Cacciabue, Hjälmdahl, Lüdtke, Riccioli, Eds., 2011) at http://mvl.mit.edu/MVLpubs/MVL_10.10_Liu_HMAT2010_Springer.pdf (last accessed Jan. 29, 2014).

able to claim that the systems meeting those tests can address the safety risks of those real-world conditions.

5. Emergency Electronic Brake Light

Emergency Electronic Brake Light addresses the Lead Vehicle Decelerating scenario and shares some overlap in functionality with the Forward Collision Warning application. EEBL warnings could improve through the use of additional information, such as lane-level information, street-level information, roadway geometry and elevation, etc. EEBL operation could be revised to include different scenarios not covered by FCW that could provide distinct benefits for EEBL compared to other applications.

6. Intersection Movement Assist

Intersection Movement Assist has the potential to address each of the crash types for real-world junction crossings. As currently implemented, the application does not issue a warning and the test metrics do not test for warnings under certain circumstances, such as when a vehicle entering an intersection is moving at low speeds. The analysis of the currently-available research has uncovered a number of limitations of the performance and test metrics.

The current test procedures should be modified to reflect a greater range of speeds and a greater variety of road geometry configurations, particularly non-perpendicular intersections, curved roads, and overpasses (a false positive test) to allow for extended safety benefits to be claimed for these crashes. A wider range of testing, especially at higher speeds (representing real-world crash speeds), will require the development of safer protocols that reduce or eliminate the consequences of a crash during testing, such as using remote guided targets as opposed to real vehicles.

7. False warning improvement research

The agency has determined that additional research to mitigate false positive warnings for the V2V safety applications identified above would be beneficial. If false positive warnings are perceived as annoying by the driver, user acceptance could decline, and driver response to true warnings might be negatively affected. This research need has been identified and work is underway to establish the research plan and conduct the necessary investigation to determine how to improve upon the performance of V2V safety application advisories and warnings through mitigating false positives.

The opposite of a false positive alert is a false negative alert. False negative alerts are also referred to as missed alerts. A missed alert occurs when two equipped vehicles are in an imminent crash situation and the associated safety application does not issue an alert. Missed alerts may result in a crash occurring that could have been avoided.

Missed alerts will be analyzed as part of the Safety Pilot Model Deployment. A preliminary FCW missed alert analysis was conducted using the first 6 months of data. The analysis identified seven possible no-alert situations that mimicked other FCW alerts situations. After further analysis of the time-to-collision, and when the subject applied the brakes; none of the situations represented a missed alert. Given the analysis was limited to a single safety application and only used the first 6 months of data, additional analysis using the full Safety Pilot Model Deployment data set will need to be completed before a determination can be made concerning the disposition of V2V missed alerts.

Research Need VI-1 False Positive Mitigation

Research Activity: Evaluation of False Positive Warning Reduction Remedies

Description: Assess the capability and capacity of possible refinements to reduce frequency of false positive warning while maintaining crash avoidance effectiveness.

Target Completion: 2016 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will leverage knowledge and experience gained during the Safety Pilot to develop various false-positive tests that exercise the ability of the DSRC-based safety systems to discern real threats from non-threat situations.

8. Performance measures improvement research

The agency also identified several areas where performance measures could benefit from additional research for each V2V safety application. This research need has been identified and work is underway to establish the research plan and conduct the necessary investigation to determine how to improve upon the performance of V2V safety applications.

The systems included in the Safety Pilot Model Deployment were designed to meet only limited CAMP test specifications and performance requirements. Accordingly, it is possible that fewer false positive warnings may have been observed during the Model Deployment if those same systems were designed to meet all of the test scenarios specified by CAMP and/or those covered by additional research testing (e.g., Track 4, IVBSS).

Research Need VI-2 Safety Application Performance Measure Rationale

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Develop a rationale to support each performance and test metric recommended for incorporation into an FMVSS.

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing certification level Safety Application Objective Test Procedures (included in the Research Need V-4 activities previously described).

Research Need VI-3 Practicability of Non-Ideal Driving Condition Testing

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Evaluate test variations for non-ideal driving conditions (e.g., curved roads, turn signal use, weather, oblique intersections) and develop a rationale supporting the inclusion or exclusion of those test conditions.

Target Completion: 2016 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

Research Need VI-4 Fused and Non-Fused V2V Safety Application Test Procedures

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Develop test procedures that can be applied to systems relying solely on V2V information as well as "fused" systems, those relying on both V2V and other sources of information (e.g., on-board sensors).

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

Research Need VI-5 Performance and Test Metric Validation

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Conduct test validation to ensure that the performance and test metrics are objective, repeatable, and practicable.

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

As a part of the agency's research, it is prudent to have real-world validation of the performance and test metrics. In other words, we would ideally have some data to indicate that systems meeting the agency's final performance requirements and test procedures in a potential FMVSS will address the safety problem as anticipated in the real world. This research need includes many components that are described above and capture in one comprehensive research activity, "Safety Application Objective Test Procedures & Performance Requirements" that has been previously described via Research Need V-4.

E. Driver-vehicle interface

While the current research-based performance and test metrics developed to evaluate the V2V safety applications are relatively robust, they do not focus on the driver-vehicle interface (DVI); an area that provides challenges not only for V2V safety but for many facets of vehicle safety devices and applications. The collaborative V2V research efforts of both CAMP and Volpe did not include the DVI as a research topic. Further, the Safety Pilot Model Deployment research was not designed to analyze and compare the different aspects of the various DVIs and, overall, the effect that specific aspects of the DVI have on safety benefits has not been clearly defined and quantified.

Other available research, such as the NHTSA Crash Warning Interface Metrics and Human Factors Connected Vehicle research projects, should yield results to help inform how the agency could proceed with more explicit guidelines or, potentially, standards for V2V DVIs. However, current available research does not yet have a method to evaluate the effectiveness of these DVI characteristics or to delineate a minimum standard for these characteristics. As a result, the DVI currently does not have performance or test metrics. Some characteristics of the DVI have research data to suggest ranges of potential performance metrics. However, these metrics were not determined considering the safety problem or a representative sample of U.S. drivers. Questions such as what are the best DVIs for particular safety applications and whether DVIs should be standardized for all vehicle types and manufacturers have not been answered.

Research Need VI-6 DVI Minimum Performance Requirements[203]

Research Activity:	V2V DVI Safety Application Study (Mini-Sim- multiple sites) and V2V DVI Characterization Study
Description:	Determine DVI's impact on effectiveness of system and safety benefits applications to establish minimum performance for crash avoidance and objective test procedures.
Target Completion:	2015

Current or Planned NHTSA research addressing this need:
This research need is being addressed by several existing projects that will result in the Development of DVI minimum performance requirements for various DVI characteristics.

[203] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

A potential regulatory action on V2V safety applications would not necessarily need to prescribe all elements of the DVI. However, at least some requirements (e.g., timing of the warning) are necessary not only to ensure that the DVI can effectively assist the driver in reacting appropriately to a crash-imminent warning, but also to ensure that warning requirements can be objectively evaluated.

F. Summary of major recommendations concerning safety applications

1) Conduct additional analysis to ensure that each performance metric is supported by a clear rationale (i.e., explain the safety risk/crash scenario that each metric is designed to address and how the metric will address that risk/scenario). The agency may need to conduct additional research to refine and validate the existing performance and test metrics against a variety of conditions under which crashes can occur.
   a) Consider the inclusion of non-V2V sources of information (radar, camera, etc.) in the development and validation process for performance and test metrics, and how to handle their operation if they co-exist on a subject vehicle.
2) Conduct additional research and analysis on Driver Vehicle Interface warning characteristics that can effectively enable drivers to react appropriately and avoid the crash.
   a) This research should consider the safety problem and a representative sample of U.S. drivers. The goal of this research should be to identify minimum DVI characteristics that are necessary.
   b) This research should also consider whether multiple warnings/alerts can occur under real-world driving conditions, how frequently they might occur, and whether it is appropriate to consider methods for prioritizing those warnings to ensure that drivers are able to interpret the warning.
3) Consider whether regulatory action on various aspects of the V2V system can/should be conducted independently (e.g., separate FMVSSs covering communications protocol/basic safety message and the available applications).
4) Conduct additional research to determine the minimum basic safety message broadcasting range and frequency that are necessary to support each V2V safety application. The minimum BSM range and frequencies found in this research would need to be considered in the implementation of a message congestion mitigation strategy (Sections V.E.1.c) and V.E.2.b)).

G. System compliance and enforcement

The Safety Pilot played a critical role in helping the agency to begin to understand what V2V system compliance and enforcement strategies and procedures might be necessary if the agency decided to proceed with rulemaking to require V2V technology. "Standing up" the Safety

Pilot environment, for example, required conducting informal certification and compliance activities to ensure that participating devices were interoperable and that safety applications were functioning according to the specifications developed for the pilot activity.

However, the kinds of compliance obligations that vehicle (and V2V device) manufacturers could face if NHTSA did proceed with rulemaking for V2V would likely be much more rigorous than anything faced by participants in the Safety Pilot. V2V devices *must be* interoperable in order for a V2V system to work properly; safety applications will not be effective if messages are not transmitted and received correctly. Assuming that the agency did decide to proceed with rulemaking, a standard requiring DSRC devices in all new vehicles would likely specify in detail (perhaps with some incorporation by reference of relevant parts of IEEE and SAE standards, which we would assume would be improved by that time to address the issues discovered during the Safety Pilot, etc.) exactly what specifications all related devices would have to meet. The agency recognizes that additional research and development is required to develop those specifications and accompanying test procedures, although we expect that much of the work completed to stand up the Safety Pilot can be leveraged as a foundation.

Research Need VI-7 Compliance Specifications and Requirements

Research Activity: DSRC Device Performance Requirements,_and Test Procedures

Description: Development of performance requirements, test procedures, and test scenarios to evaluate a device's compliance with interoperability standards, security communication needs; and to support safety applications.

Target Completion: Onboard requirements (mid 2015), and draft test procedures (late 2015). Candidate performance requirements, test procedures, and test scenarios identified (late summer of 2015).

Current or Planned NHTSA research addressing this need:

The research need is addressed through activities previously described under Research Needs V-2 and V-3. This research will identify the initial level of performance requirements, test procedures, and test scenarios that will facilitate evaluating the compliance of DSRC devices.

Once NHTSA establishes a FMVSS, vehicle and device manufacturers would be required to certify that they comply with it in order to sell vehicles and devices. Non-compliance with a FMVSS could result in enforcement action by NHTSA (e.g., a requirement to recall affected vehicles and devices, an injunction from selling affected vehicles and devices until remedied, civil penalties). Additionally, if V2V devices develop a safety defect, manufacturers (both of vehicles and V2V devices) may also be subject to a recall. It is possible that manufacturers may choose to rely on some kind of third-party certification for V2V devices to ensure uniform adherence to NHTSA's requirements, but NHTSA would not expect to participate in that certification.

NHTSA may need to conduct further research into how to ensure that all V2V devices subject to a recall can be located, given the possibility that some devices may be mobile and go from vehicle to vehicle or owner to owner. Section VIII.B.3 discusses the possibility that for vehicles manufactured with V2V devices installed, the SCMS may be able to create a link at the time of manufacture between specific installed V2V devices or production lots of devices and enrollment certificates that later may help vehicle manufacturers and NHTSA identify defective V2V equipment. NHTSA worked with CAMP to identify and document alternative approaches that could be implemented to link device batches to enrollment certificates. However, it is not yet clear how such a linkage would be created for V2V devices that are not installed by the manufacturer, an important enforcement matter for NHTSA should the standards include aftermarket equipment.

VII. Public Acceptance

A. The importance of public acceptance

The Safety Act requires that FMVSSs issued by the agency be practicable, and an important part of that consideration is whether the public is expected to accept and correctly use the technologies installed in compliance with the standard. According to the case law, a standard issued by the agency will not be considered practicable if the technologies installed pursuant to the standard are so unpopular that there is no assurance of sufficient public cooperation to meet the safety need that the standard seeks to address.[204] Crash avoidance technologies in general, and V2V in particular, are new to consumers, and new technologies that can dramatically change the driving experience always have the potential to raise public acceptance issues. For V2V technologies, the extent to which the public understands and embraces the enhanced level of safety (and other mobility and environmental benefits) made possible by a V2V environment will need to outweigh the risks to individual privacy, actual or perceived, introduced by these technologies. Additionally, as a practical matter if not a legal one, industry acceptance and cooperation may be equally important, should NHTSA take steps to regulate V2V technologies via FMVSS, particularly since NHTSA is hopeful that industry will play a central or supporting role in establishing key components of the SCMS, which is required to support deployment of V2V technologies.

1. Potential key aspects of consumer acceptance for V2V communication

a) Enhanced levels of safety

V2V technologies can potentially provide considerable safety benefits, but consumers are more likely to accept V2V technologies quickly if they understand *how* vehicles with this technology can be safer. Crash avoidance technologies play, at first glance, a more abstract role in keeping consumers safe than crashworthiness features. If a driver avoids a crash, it may be difficult for the driver to detect whether it was the driver's own skill or the on-board technology that actually "saved" them, as compared to a crashworthiness technology like air bags, which clearly deploy to protect the driver and occupants in a crash. Consumers who cannot clearly see benefits to V2V technologies could be more tentative in their acceptance of V2V for longer than they might be with other safety technologies. Performing outreach to educate consumers on the safety benefits of V2V technologies, as well as on the privacy-protection methodology built into the V2V communications system, will likely be helpful to improving consumer acceptance, should the agency move forward with regulation. Some possible methods of public outreach

[204] *Pac. Legal Found. v. Dept. of Transp.*, 593 F.2d 1338, 1345-46 (D.C. Cir.), *cert. denied*, 444 U.S. 830 (1979).

include working with industry to produce and air Public Service Announcements (PSAs) and conducting publicly-accessible – and media-covered -- technology demonstrations with V2V-enabled vehicles nation-wide.

Preliminary research from the auto industry, however, seems to indicate that at least some members of the public would be interested in V2V-type technologies on their vehicles. On June 5, 2013, at the Telematics Detroit Conference, the Alliance of Automobile Manufacturers released poll results finding that a majority (59 percent) of consumers "believe that technological innovations such as driver-assist technologies are making cars safer, and 6 in 10 consumers want to check out these systems next time they buy a car."[205]

b) Security from new forms of cyber-attack

With increasing frequency, legislators and the media have raised questions about whether the prevalence of electronic control in today's high-tech motor vehicles has created new vectors (or sources) for cyber-attack on the motoring public. For example, during a hearing in 2013, Senate Commerce Committee Chairman Jay Rockefeller asked, "As our cars become more connected -- to the Internet, to wireless networks, with each other, and with our infrastructure -- are they at risk of catastrophic cyber-attacks?"[206] To date, NHTSA's V2V research has not included research specific to this issue, as researchers assumed that the possibility of cyber-attacks on motor vehicles was an existing vector of risk – not a new one created by V2V technologies. However, should the agency move forward with regulation, it may be important for improving public acceptance of the technology for us to assess, specifically, whether and how V2V technologies augment existing – or create additional – paths of cyber-attack that may affect motor vehicle security. The agency may also wish to explore the availability and appropriateness of measures to mitigate cyber-attack risks specific to V2V technologies (if any exist). Additionally, efforts to achieve consumer acceptance through public outreach and education on the benefits of V2V technologies may help to assuage public concern that V2V technologies will increase the danger of cyber-attacks on motor vehicles.

In the June 5, 2013, poll released by the Alliance mentioned above, it was also found that consumers, when questioned about self-driving vehicles, expressed concerns about cyber-security (i.e., 81 percent about a computer hacker controlling the car), companies collecting data from the self-driving cars (i.e., 75 percent), and companies sharing this information with the government (i.e., 70 percent). It is important to note that consumers were responding about self-

[205] Consumers Still Want to Be in the Driver's Seat, Self-Driving Cars Raise Concerns (Poll on Alliance Web site, June 5, 2013) at www.autoalliance.org/INDEX.CFM?OBJECTID=156688B0-CD5D-11E2-8898000C296BA163 (last accessed Jan. 29, 2014).

[206] U.S. to monitor cybersecurity risks as car connectivity grows (Automotive News, May 15, 2013) at www.autonews.com/article/20130515/OEM11/305159928#axzz2Z1OdGToG (last accessed Jan. 29, 2014).

driving vehicles and not about V2V communication specifically,[207] but their concerns about cyber-security and collection of data about their driving behavior are concerns that consumers could have regarding any sort of vehicle for which they believed could present such risks.

While the agency recognizes the difference in potential risk between V2V technologies that simply warn drivers about impending danger and technologies that actually intervene in driving, this distinction may not yet be so clear to consumers, and work could be done to make that distinction clearer to improve public acceptability of V2V (ideally without also negatively impacting acceptability of more advanced technologies).

c) Reasonable cost increases

Another component of consumer acceptance is cost. The extent to which consumers are willing to embrace V2V technologies will depend, in part, on the resulting cost increase in new motor vehicles. Generally speaking, cost as an issue for consumers has been considered in terms of whether it is high enough to cause many consumers to delay purchasing a new vehicle. It is not an issue that has been raised very often – but, if consumers delay purchasing of new vehicles in any significant way, presumably there will be a delay in the stream of expected benefits. This is an issue that the agency considers for any safety regulatory action that it undertakes.

The preliminary costs for V2V (initial cost estimated at about $350 and then decreasing with the learning curve) are less than some of the more notable safety equipment. For example, frontal air bags for the driver and right front passenger are estimated to cost $496, and antilock brake systems are estimated to cost $424 (all in 2012 dollars).

d) Privacy protection and acceptable levels of risk to exposure

Perhaps the most significant component of consumer acceptance in the V2V context will be the extent to which V2V technologies create consumer anxiety about risks to individual privacy, whether the risks are actual or simply perceived. As discussed below, if consumers believe—contrary to the actual facts-- that the V2V system as contemplated will enable the government or others to track the speed or location of their motor vehicles, the public may be less likely to support a regulatory mandate requiring the technology, regardless of any resulting enhancements to levels of safety.

Should the agency move forward with a V2V regulation, it will need to perform and make public a privacy impact assessment (PIA) of its proposed V2V FMVSS. Discussed in detail in Section VII, a PIA must capture and quantify all privacy risks introduced by proposed regulatory requirements, and assess the extent to which technical, physical and organizational controls designed to minimize such risks do so adequately. Once complete, the PIA will enable

[207] See Section VII.A.3.b) for NHTSA's current findings on driver responses to similar topics in the Safety Pilot.

NHTSA (and DOT as a whole) to determine whether the level of residual risk to individual privacy, with all controls in place, is acceptable.

A critical part of any efforts to achieve consumer acceptance through public outreach will be assuring consumers that V2V technologies do not pose a significant threat to privacy and have been designed to help protect against vehicle tracking by the government or others. Additional privacy research and analysis (some of which will be folded into the agency's planned security and privacy risk assessments) is expected to provide NHTSA and DOT with an even more substantial basis for making such public assurances than currently exists.

2. Potential issues With industry support for V2V communication systems

Support from the automotive industry is not legally required in order for NHTSA to move forward with regulating V2V technology, but it is certainly desirable from a policy perspective, and may be important if the agency anticipates that the security system would be developed and stood up by an industry consortium. Industry support may be hindered by concerns about costs associated with the security system required to support V2V communications – who will bear the burden of such costs and, to the extent that it is the consumer, whether V2V can offer any "day one" benefits to consumers that justify the increase in new vehicle costs resulting from regulation of V2V technologies. Industry support also may be impaired both by uncertainty about how a regulatory action might impact in-vehicle crash avoidance systems, and by the perception by industry that V2V technologies will result in increased legal liability.

Additionally, for what appear to be largely economic reasons, industry support also will turn, in part, on the extent to which V2V technologies create consumer anxiety about actual *or perceived* risks to individual privacy. Industry members, through the VIIC and individually in meetings with NHTSA, have expressed concern that consumers will opt not to buy new vehicles if the agency mandates V2V technologies without protecting consumer privacy to the extent industry believes is necessary, and without providing consumers with assurances of privacy protection in a very public way, as through PSAs and public outreach.

Industry also may be able to use suggestions from the agency on how to facilitate consumer acceptance of V2V technologies if the agency eventually decides to require them. In addition to privacy, another factor that can be relevant to public acceptance of technologies is how well they work over the vehicle's lifetime. As discussed elsewhere in this report, we anticipate that BSMs will need to be accompanied by security certificates to establish their trustworthiness; if vehicles need to be resupplied periodically with certificates, or if vehicles need software upgrades regularly (or even occasionally), there may be consumer acceptance issues if receiving these certificates and upgrades requires what they consider to be undue effort or expense on their part. At the same time, however, if consumers reject the effort or expense, the systems may not function properly, which can cause other consumer acceptance issues. Ensuring appropriate consumer participation in V2V system maintenance will be a topic that the agency continues to explore.

3. Preliminary information on consumer acceptance

As part of its research thus far, the agency has accumulated some preliminary information on consumer acceptance of advanced crash avoidance systems (sensor-based and V2V-based).[208] This information provides an early look into consumer concerns and their perceptions on the value of these types of systems.

Based on our preliminary research described above, drivers generally have some interest in the new crash avoidance technologies, even if they do not yet have extensive knowledge about them. Consumers who have driven vehicles with crash avoidance technology appear to be generally positive about this technology, regardless of whether the technology is sensor-based or V2V-based. Exposure to specific crash avoidance technologies seems to increase drivers' interest in purchasing those same technologies in future vehicles.

However, even though consumers express interest in purchasing vehicles with crash avoidance technologies, public opinion polls do not show that drivers are willing to spend a lot of additional money in order to purchase vehicles with these systems. In contrast, there is some indication that use of currently-available crash avoidance technologies has resulted in reduced claims/losses for the owners of vehicles with these features.[209] If this trend continues and drivers determine that the new technologies can reduce their insurance costs, they might be willing to increase the amount of money they are willing to pay for a vehicle with crash avoidance technology.

The agency intends to supplement its preliminary research in the areas of consumer acceptance of V2V technology to better understand consumer behavior in reaction to these technologies. This research would help inform approaches for system implementation if the agency decides to move forward with a regulatory action.

[208] Independent Evaluation of the Driver Acceptance of the Cooperative Intersection Collision Avoidance System for Violations (CICAS-V), Pilot Test July 2011, (Stearns and Garay-Vega, Report No. DOT HS 811 497) and Integrated Vehicle-Based Safety Systems (IVBSS) Field Operational Test Final Program Report (Sayer, et al., June 2011, Report No. DOT HS 811 482) both at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 29, 2014).

[209] More good news about crash avoidance, at 1-4 (Insurance Institute for Highway Safety, 2013, Status Report 48 (3)) at www.iihs.org/externaldata/srdata/docs/sr4803.pdf (last accessed Jan. 29, 2014).

Research Need VII-1 Consumer Acceptance[210]

Research Activity: Consumer Acceptance Research on V2V
Description: Supplement the driver acceptance analysis completed per the Driver Clinics and Safety Pilot Model Deployment with further research that includes a focused assessment of privacy in relation to V2V technology
Target Completion: 2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:
NHTSA will initiate Consumer Acceptance research in 2014.

a) Driver clinics conducted for connected vehicles and applications

As part of the V2V Light Vehicle Driver Acceptance Clinics project (conducted from September 2010 to March 2013), some preliminary assessments were made about whether and how drivers accept and respond to V2V safety technology. Beginning August 8, 2011, and ending January 21, 2012, four-day driver acceptance clinics were held in six cities,[211] with driver recruitment being conducted by independent recruitment agencies that used existing databases of known interested parties, advertisements, and/or cold-calling. At each clinic, around 112 drivers participated in a structured exposure to the V2V technology.[212] This exposure included completing pre-and post-drive questionnaires, receiving an oral and a video briefing about V2V technology, and being oriented to the vehicles and the course that would be driven. Clinic vehicles were supplied by nine OEMs, one from each OEM. Not all of the applications being assessed were included in each of the vehicles. In order for all of the participants to experience the majority of the safety features, some of the participants were asked to drive two different vehicles.[213] In addition, 104 drivers at each clinic participated in a focus group discussion about the V2V technology and their experience in driving these vehicles.[214]

[210] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

[211] Brooklyn, Michigan; Brainerd, Minnesota; Orlando, Florida; Blacksburg, Virginia; Fort Worth, Texas; and Alameda, California.

[212] Specifically, the EEBL, FCW, BSW/LCW, DNPW, IMA, and LTA applications.

[213] Participants driving the Ford, GM (Cadillac), Honda (Acura), or Mercedes were not asked to switch vehicles. Those driving the Toyota switched halfway to the Hyundai, and vice-versa, with similar switches being made between the Nissan (Infiniti) and the VW/Audi vehicles.

[214] Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot [V2V-SP], Draft Final Report, Volume 1: Driver Acceptance Clinics (April 10, 2014). See Docket No. NHTSA-2014-0022.

Key findings from the pre- and post-questionnaires[215] completed by drivers at these clinics include:

- Overall Impressions: Overall impressions of the V2V vehicles were positive, with approximately 85 percent of all responses considered to be positive. The most frequent negative response, accounting for only 4 percent of all responses, was a general "disliked the warning."

- Effectiveness: the majority of comments were positive regarding how effective the issued alerts were at communicating the direction of the scenario-specific threat (i.e., approximately 60 percent positive, with 22.5 percent giving a neutral response).

- Desirability: the desirability of the safety features was extremely high with 90 percent of participants agreeing that they would like to have the V2V communication safety feature in their personal vehicle.

- Intuitiveness: the intuitiveness of the vehicle's alerts was rated very high (i.e., approximately 89 percent of respondents felt that the alert issued was extremely effective at gaining their attention and directing attention to the threat. Similarly, 90 percent agreed that the alert issued was easy to understand.).

- System Limitations: Most respondents (61.1 percent) were unsure whether or not drivers might confuse one warning with another from a different safety feature, while 30 percent did not think this would be an issue.

- The majority of respondents (90.5 percent) would want to be notified whenever the V2V communication became unavailable; however, 43 percent of respondents stated that they would accept an unavailability rate of 10 percent or lower.

- The majority of respondents do not believe that the V2V benefit would be noticeable until 70-80 percent of vehicles are similarly equipped.

Some overall reactions by focus group members about V2V include:

- "Standard on all vehicles" was far preferred to the term "mandatory," which some respondents perceived as too controlling. Participants felt that communication efforts

[215] Safety Pilot: Preliminary Analysis of the Driver Subjective Data for Integrated Light Vehicles (Scott Stevens, July 2013, HS63A3 – Project Memorandum). See Docket No. NHTSA-2014-0022

around the system should avoid the word "mandatory" or other terms implying government control, but could use terms such as "your own personal co-pilot."

- Participants tended to agree that the benefits of saving lives and preventing or mitigating crashes far outweigh potential drawbacks such as driver dependency, complacency, and over-reliance on the system.

- Participants considered the scenarios experienced during the driving portion of the clinic as being very relevant and applicable to their everyday driving experiences.

- The applications considered the most appealing and/or relevant overall were FCW, BSW, EEBL, and IMA, although there was slight variation of this depending upon the region of the country that the respondent lived.

- Participants felt there were near-term problems (e.g., texting, disregard for rules, poor driving) that need to be addressed before starting a new, complicated, interdependent technology, even though there did not appear to be any short-term solutions in identified for these near-term problems.

- Participants' reactions to the various warning implementations used by the OEMs (e.g., visual, audible, haptic where present and the locations thereof) were mixed, but there was a fair amount of consensus around having the warning appear the same across OEMs to avoid confusion when driving different vehicles.

b) Model Deployment driver acceptance surveys

As part of the Safety Pilot Model Deployment project, assessments were made to determine whether and how drivers accept and respond to V2V safety technology. The V2V technology with which these vehicles were equipped included six safety applications that were developed to assist the drivers in avoiding risky situations that might result in a crash if the driver did not take corrective action: EEBL, FCW, BSW/LCW, DNPW, IMA, and LTA,[216] although not all of the applications being assessed were included in each of the vehicles.

During the first 6-month period (i.e., August 2012 to February 2013), half (i.e., 64) of the participants drove the vehicles, and, at the end of that 6-month period of time, filled out the driver acceptance survey. The remaining 64 drivers began driving the same OEM-provided and equipped vehicles at the beginning of the next 6 months of the pilot (i.e., February 2013), and

[216] See id., at 5, Table 1 for additional information on the safety features that were available by OEM.

they filled out the same driver acceptance survey at the end of the next second 6-month period of time (i.e., August 2013).

A preliminary analysis was conducted on the subjective survey data obtained from the drivers who drove the V2V-equipped vehicles for the first 6 months, and was reported in a July 2013 draft report. Overall, driver's responses were very mixed toward the V2V safety features, with a large proportion of drivers giving neutral responses. Their responses to "What did you like most about the Connected Vehicle system?" included "Alerted me to traffic situations I otherwise wouldn't have been aware of," but the drivers focused on the rate of alerts that they regarded as incorrect, with 42 percent citing incorrect alerts (e.g., distracting, not always clear, too short in duration), when asked what they like least.[217] Especially in regard to FCW, the false alerts appeared to have some effect on desirability of the FCW safety feature. The more false FCW alerts a driver believed they had received, the less they agreed with the statement, "I would like to have FCW on my personal vehicle."[218]

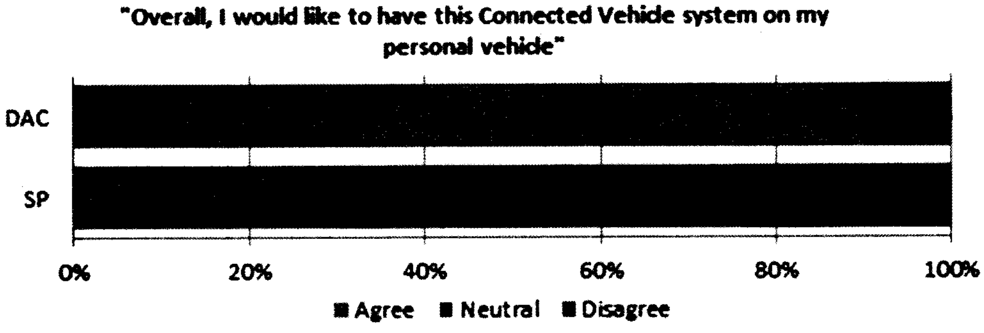
Since many of the driver survey questions that were used in the Driver Acceptance Clinics were used in the Safety Pilot Model Deployment, a comparison of results is possible. However, the light vehicle Driver Acceptance Clinics were staged demonstrations of the V2V technologies that were conducted using integrated vehicles by each of the eight OEMs between August 2011 and January 2012. The volunteers drove equipped vehicles on a closed course through a series of staged scenarios designed to illustrate how the different safety features could be of use, and only interacted with other vehicles driven by professional drivers. The main difference was the overall distributions of answers to the questions asked, with almost all drivers giving the highest rating for every system and question for the Driver Acceptance Clinics, whereas responses in the Safety Pilot Model Deployment were largely neutral. These results are not surprising given the differences in environment with the Driver Acceptance Clinics, a controlled demonstration, as compared to the Safety Pilot Model Deployment, a real-world driving situation. Table VII-1 and Figure VII-1 provide a sample of the distribution of driver responses.

[217] Id., at 9.
[218] Id., at 36.

Table VII-1 Comparison of Findings between Driver Acceptance Clinics and Safety Pilot Model Deployment during the First 6 Months

	Driver Acceptance Clinics	**Safety Pilot Model Deployment (Phase 1 Drivers)**
Would like to have V2V technology on their personal vehicle	91%	30%
Most highly rated safety feature	IMA	BSW/LCW
Said distraction was less than using car radio	75%	51%
Thought the system would not cause overreliance	42%	73%
Amount young drivers worried about overreliance compared to older drivers	more	Less
Main gender difference was	Higher ratings for the **EEBL** by women (more useful, desirable, effective, and understandable)	Lower ratings for the **IMA** by women (less desirable, effective, understandable, and with more incorrect alerts)
Generally more favorable ratings for the overall system from older drivers in both, especially for the **EEBL** (higher ratings of **FCW** among older drivers only seen in Safety Pilot Model Deployment)		

Figure VII-1 Full comparison of DAC and SP Driver responses



Upon completion of the Safety Pilot Model Deployment, the total data set, including the data from the second 6 months, will be analyzed to confirm the findings in this report. Since some changes were made to the safety applications that affected the false warning rates (i.e., decreased the number of false warnings), this analysis could prove to be very useful, in examining the rate and amount of change of a driver's opinion about a V2V safety application as the false warning rate decreases. Information gained from this analysis can be used to judge future driver opinions of V2V safety applications, as the applications are improved, based upon the information obtained in the Safety Pilot Model Deployment.

Preliminary indications are that driver acceptance of the IMA application improved in the last 6 months of the project. This improvement in driver acceptance correlates with the enhanced performance of the IMA application as a result of changes by the OEMs to address the sources of concern, especially what were perceived as false warnings. Generally, the applications used in the Model Deployment were not fine-tuned to suppress false warnings in situations where production systems would. Continued refinements, to the extent possible for IMA and other V2V applications, may help address some of the concern without affecting the effectiveness of the systems.

The survey also attempted to gauge participants' concern with regard to privacy issues through four questions: "How willing would you be to have Connected Vehicle technology on your vehicle that, when combined with other information may allow:

A) A business entity to learn about your vehicle's location and travel patterns?

B) The government to learn about your driving behavior and patterns?

C) A third party organization to learn about your driving behavior and patterns?

D) Appropriate personnel to determine criminal behavior such as hacking?

Note that these questions were intended to address possible perceptions, not the reality of the contemplated system, which is not designed to permit the collection of the types of data referred to in questions A through C.

In response, drivers did express concern about privacy with V2V technologies, with over half declaring that they were "not willing" to have businesses, government, or a third party organization learning about their driving behavior and patterns. When the idea of criminal behavior such as hacking was introduced, this number fell to 28 percent, indicating more people would be willing to accept some level of tracking. This is the clearest expression that the agency currently has of driver opinions of V2V privacy issues when drivers have actually experienced V2V technology over an extended period of time. While a larger sample set would be more informative, these results indicate that this is an issue that the agency needs to consider carefully as implementation proceeds.

VIII. Privacy Considerations

A. Privacy considerations – what they are and why they are important

Risks to consumer privacy, whether actual or perceived, are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about whether and, if so, how to proceed with V2V research or regulation.

At the outset, readers should understand some very important points about the V2V system as contemplated by NHTSA. The system will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V security system that could be used by law enforcement or private entities to personally identify a speeding or erratic driver. The system—operated by private entities—will not permit tracking through space or time of vehicles linked to specific owners or drivers or persons. Third parties attempting to use the system to track a vehicle would find it extremely difficult to do so, particularly in light of far simpler and cheaper means available for that purpose. The system will not collect financial information, personal communications, or other information linked to individuals. It will enroll V2V enabled vehicles automatically, without collecting any information identifying specific vehicles or owners. The system will not provide a "pipe" into the vehicle for extracting data. The system will enable NHTSA and motor vehicle manufacturers to find lots or production runs of potentially defective V2V equipment without use of VIN numbers or other information that could identify specific drivers or vehicles.

Generally, privacy considerations inherent in mandated V2V technologies include such issues as:

- Should the V2V system provide "anonymity"[219] for drivers, as suggested by industry, in order to prevent location tracking and otherwise protect individual privacy?
- Should the V2V system provide "anonymity" for drivers *even if* doing so:
  - Prevents identification and prosecution of hackers accessing computers or data on the V2V system without authorization?

[219] The VIIC has defined "real anonymity" as "end-to-end anonymity" (i.e., no collection of any personally-identifying information at any time in connection with bootstrapping or provision of security services or mandatory applications). By contrast, NHTSA avoids use of the term "anonymity" in the V2V context, in recognition of the fact that some limited risks to individual privacy exist in the current V2V design even through it does not provide for collection of any individually identifying information.

    - Impedes NHTSA's ability to investigate and recall defective V2V motor vehicle equipment (i.e., for highway safety purposes)?
- Or, for system security and/or highway safety purposes, should the V2V system collect data that may link location or other information that drivers may potentially perceive as sensitive (e.g., speed) to an individual driver or vehicle, either directly or indirectly?
- Are there ways to satisfy NHTSA's need to identify potentially defective V2V devices without collecting data that may link location or other potentially sensitive information (e.g., speed) to an individual driver or vehicle, either directly or indirectly?
- Can a V2V system with no mechanism for identifying or tracking down hackers or other "bad actors" be sufficiently secure for NHTSA or consumers to rely on?
- What specific risks to privacy stem from the V2V system? How likely is the potential occurrence of such risks? What would be the extent of harm if the events occurred? For example, to what extent do either the SCMS design or the unencrypted BSM introduce privacy risks, including but not limited to the risk of location tracking?
- What physical or technical controls should the V2V system contain to mitigate location tracking and other privacy risks "by design"?
- What policy or organizational controls should the V2V system contain in order to minimize the likelihood of unauthorized access to insider information that could facilitate tracking or create other risks to privacy?
- What role, if any, *should* or *can* the Federal Government play in assuring individual privacy in connection with mandated V2V technologies – especially if it plays no role in owning or governing the SCMS?
- Is Federal legislation necessary to protect consumer privacy adequately in the context of a mandated V2V FMVSS, as suggested by CAMP and the VIIC?

1. Transmission, collection, storage, and sharing of V2V data

There are two primary categories of V2V system functions that involve the transmission, collection, storage, and sharing of V2V data by, and between, the V2V system components and other entities: system safety and system security.

The V2V system's safety functionality (i.e., the safety applications that produce crash warnings) requires that V2V devices in motor vehicles send and receive a basic safety message containing information about vehicle position, heading, speed, and other information relating to vehicle state and predicted path. The BSM, however, contains no personally identifying information (PII) and is broadcast in a very limited geographical range, typically less than 1 km. Nearby motor vehicles will use that information to warn drivers of crash-imminent situations. Except in the case of malfunction, the system will not collect and motor vehicles will not store the messages sent or received data sent/received by V2V devices.

The security needs of the V2V system require the exchange of certificates and other communications between V2V devices and the entity or entities providing security for the V2V system (i.e., the Security Certificate Management System). These two-way communications are encrypted and subject to additional security measures designed to prevent SCMS insiders and others from unauthorized access to information that might enable linkage of BSM data or security credentials to specific motor vehicles.

NHTSA also needs to ensure that the V2V system is protected from defective devices. This agency safety function is likely to require that the V2V security system collect and share, on a very limited basis, some V2V data linking V2V device production lots to security credentials. Neither the V2V system nor NHTSA will collect, store or have access to information that links production lots of defective V2V devices with specific VINs or owners.

2. Privacy policies framework

Industry members, via CAMP, the VIIC, and in individual OEM meetings with NHTSA, have suggested that the Federal Government should play a central role in protecting individual privacy in the V2V context, through regulation or governance over the SCMS. Both CAMP and the VIIC have taken the position that the security system for V2V technologies should conform to the central tenets of the VIIC Privacy Policies Framework (version 1.0.2), dated February 16, 2007. That document would require that the security system:

- Collect and transmit only "anonymous" data from mobile users for mandatory applications
- Keep such data "anonymous" until securely destroyed
- Collect PII only with consent of the consumer
- Use/transmit that PII only in ways to prevent misuse/leakage and unauthorized attacks on the system

On the basis of these general tenets, the VIIC has identified as specific security system requirements:

- End-to-end anonymity for privately owned/leased vehicles and occupants for all mandatory V2V technologies, including security system processes (bootstrapping and certificate distribution) and mandatory applications and services
- For mandatory services, no ability to track specific identified vehicles across space and time, concurrent or after-the-fact
- Protection from attacks on system integrity, including from hackers and system administrators (i.e., "insiders"), by:
  - Providing secure, end-to-end encryption of vulnerable communications;
  - Changing short-term security certificates and vehicle identification every few minutes to prevent location tracking;
  - Assigning certificate signing requests (CSRs) - now called Enrollment Certificates or Long-term Certificates -- in an anonymous fashion;

- Providing for multiple, legally/administratively separate SCMS entities with distinct governances, none of which have sufficient knowledge, information, or means necessary to link short-term certificates to CSRs/Enrollment Certificates and ultimately to vehicles/OBE, all of which should be prohibited "by law" from allowing or colluding to achieve re-identification;
- Providing sufficient security to prevent hackers, users, and system administrators from accessing or deriving any information that can be linked, directly or indirectly, to individuals, motor vehicles, or OBE (e.g., via VIN or vehicle-specific part numbers).

CAMP and the VIIC also have taken the position that Federal legislation implementing the Privacy Policies Framework (as well as other policy and technical aspects of DSRC deployment) is necessary to provide adequate privacy protections for consumers in the context of mandated V2V technologies.

NHTSA takes privacy very seriously. If NHTSA moves forward with regulating V2V technologies, we are committed to doing so in a manner that both protects individual privacy and promotes this important safety technology. In NHTSA's view, the VIIC's 2007 Privacy Policies Framework provided an initial framework and useful starting point for development of privacy-protective V2V technologies. However, both V2V technologies and policies impacting privacy have continued to evolve over the last six years. Additionally, since 2007, DOT and V2V stakeholders have identified mission-critical and system-specific safety information needs that affect system privacy and have necessitated development of various additional controls to mitigate adverse privacy impacts. For these reasons, some aspects of the tenets and specific requirements set forth in that document no longer may be viable.

For example, in order to preserve anonymity and prevent tracking, the 2007 Privacy Policies Framework envisioned the creation/collection of no data whatsoever that could link a security certificate that authenticates a V2V message to the on-board device or motor vehicle that generated that message. However, as discussed below, in order for NHTSA to investigate and ensure the recall of defective V2V equipment, the security system must collect/store data that facilitates linkage between some categories of misbehavior reports (to be identified as the misbehavior functions mature) and the production lots of V2V equipment that generated those messages. Without collection by the SCMS of such information, NHTSA will not have an adequate basis on which to ensure the system's protection from defective devices.

As detailed below and elsewhere in this report, by design, V2V devices will transmit safety information in a very limited geographical range. Nearby V2V devices will use that information to warn drivers of crash-imminent situations. As currently designed, the system and V2V devices do not intend to collect or store the contents of messages sent or received. However, in the case of malfunctions, a limited number of BSM elements relevant to assessing performance will be stored, but in a manner designed to preserve personal privacy to the maximum extent possible, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread.

We have worked closely with CAMP and the VIIC to develop a technical and policy approach that helps guard against risks to individual privacy. As conceived, the system will contain multiple technical, physical, and organizational controls to minimize privacy risks – including the likelihood of vehicle tracking by individuals and government or commercial entities. Additionally, even though V2V is still in a research phase, DOT's Chief Privacy Officer and Office of the General Counsel and NHTSA's Offices of the Chief Counsel and Chief Information Officer have worked closely with the DOT research team throughout the life of the project to identify and assess the privacy implications of the V2V system and DOT's related mission needs. For example, DOT's Privacy Officer worked with the Office of the Chief Counsel of OST-R and the Office of the General Counsel to publish a Systems of Records Notice covering collection of personally identifying information during the Safety Pilot and, in so doing, identified appropriate controls to mitigate risks to individual privacy associated with that effort.[220] These offices also supported the NHTSA's V2V team in its initial assessment of the possible privacy risks associated with the V2V system (detailed below).

As aspects of the V2V system (such as the misbehavior functions, communications media, and ownership/governance models) become more defined, NHTSA will continue to work with the Department's Privacy Officer and Office of the General Counsel to assess and reassess any threats to privacy that may be introduced by V2V technology and help identify mitigation measures to minimize any such risks. Additional discussion of NHTSA's interim privacy risk assessment and next steps can be found in Section VIII.B.

3. The fair information practice principles

DOT and NHTSA privacy assessments are based on the framework of the fair information practice principles (FIPPs). Rooted in the tenets of the Privacy Act, the FIPPs provide a foundation for the privacy laws of multiple States, Federal and international governments, and organizations. A FIPPs-based analysis is predicated on privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council, and the Privacy Controls, articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

[220] 77 Fed. Reg. 12641 (Mar. 1, 2012) at www.gpo.gov/fdsys/pkg/FR-2012-03-01/pdf/2012-4964.pdf (last accessed Jan. 30, 2014).

The control families consist of:

- **Transparency**: What mechanisms will provide the consumers with information about the data being collected and transmitted by the V2V system and how that data will be used?
- **Individual Participation and Redress**: Will consumers have a reasonable opportunity to make informed decisions about the collection, use, and disclosure of their PII, if collected, or other data that may be used to identify them, directly or indirectly? Will they be active participants in decisions regarding the collection and use of their data?
- **Purpose Specification**: For what purposes is the system collecting, using, maintaining, or disseminating the specific data elements or categories of data being collected? (for example, here is where NHTSA might indicate that V2V data collected by roadside infrastructure will be aggregated, de-identified, and transmitted for use in mobility, environmental, and/or commercial applications)
- **Data Minimization**: Explain why the data collection isn't excessive and how long the data will be retained
- **Use Limitation**: Assure the subjects of the data collection that the data will not be used for purposes incompatible with the purpose for which it was collected (as detailed in the purpose specification section)
- **Data Quality and Integrity**: How will the system assure data quality and integrity throughout the data lifecycle and in all business processes associated with data use?
- **Security**: What physical, technical and procedural measures will system administrators take to protect the data? The PIA's analysis of security controls in the security system that mitigate privacy risks should be specific enough to provide consumers with a comprehensive understanding and adequate assurance that information is protected – but not provide a roadmap for would-be hackers to attack the system.
- **Accountability and Auditing**: How does system ensure that the privacy controls outlined above are executed?

The answers to these questions and the specific controls that NHTSA will need to identify and require, if consistent with our legal authority, within each of the control families, will flow from a technical privacy risk analysis of the V2V system. This analysis will be conducted once now-fluid aspects of the security system design (e.g., misbehavior management) are closer to finalization, once the agency knows how the SCMS will be managed (e.g., owned, organized, and operated), and once the agency knows what communications media will be selected by the SCMS owners for messaging between the SCMS and V2V devices.

A draft Privacy Impact Assessment (PIA), based on the agency's technical risk analysis, would need to be completed and ready for publication concurrent with any NPRM that NHTSA may issue, should it move forward with regulatory action. A PIA is an analysis required by the E-Government Act of how the V2V system handles information in identifiable form[221] to:

- Ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and,
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[222]

The draft and final PIA will document how DOT has considered and analyzed privacy from the beginning stages of the V2V system's development throughout the system's life cycle (i.e., collection, use, retention, processing, disclosure, and destruction). The PIA also gives the public notice of this analysis and helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions.

In order to conduct this comprehensive privacy risk assessment of the V2V system as part of a V2V regulatory action, NHTSA will need to identify and quantify the level of any privacy risks stemming from each of the three discrete areas of the V2V system -- the OBE/DSRC messages, the communications media for messaging between the SCMS and V2V devices, and the SCMS. Although a PIA cannot be finalized until a draft NPRM exists, most of the technical analysis can be completed well in advance of that time. The next section describes NHTSA's work on a PIA to date.

B. NHTSA's interim privacy risk assessment

NHTSA, with the support of the DOT Privacy Officer and NHTSA's Office of the Chief Information Officer, conducted an interim privacy risk assessment of the V2V system. As multiple aspects of the system design remain in flux, the initial privacy risk assessment was

[221] The E-Government Act of 2002 applies to "information in identifiable form." The National Institute of Standards and Technology (NIST) has stated that the term "information in identifiable form" is "[o]ften considered to have been replaced by the term PII [personally identifiable information]." See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Appendix C (April 2010, NIST Special Publication 800-122) at www.nist.gov/manuscript-publication-search.cfm?pub_id=904990 (last accessed Jan. 29, 2014). However, NIST also notes that terms such as "information in identifiable form" are similar to NIST's definition of PII and "organizations should not use the term PII (as defined in this report) interchangeably with these terms and definitions because they are specific to the ir particular context." Id.

[222] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003, OMB Memorandum, M-03-22, Attachment A, Section II.A.6) at www.whitehouse.gov/omb/memoranda_m03-22 (last accessed Jan. 29, 2014).

based on a "snapshot" of the V2V system envisioned by the CAMP/DOT research team. In addition, this assessment assumed that SCMS would have one important additional capability (not a part of the prototype security system design) required to address NHTSA's need for information to support its defect investigation and recall duties.

The initial privacy risk assessment contains an important caveat, namely, that *further development of the technology or organization of the V2V system is likely to result in changes – possibly significant changes -- to the interim privacy analysis and findings.* For this reason, the interim assessment was intended to provide the structure and serve only as a robust starting point for NHTSA's definitive assessment of risks to privacy that could stem from a V2V regulatory action. As the V2V system and NHTSA's procedural posture evolve, so too will the scope of and detail in this privacy assessment.

The primary system components analyzed were:

1. The **OBE and BSM** – On-Board Equipment (OBE) as well as BSMs containing unencrypted GPS/location data required for V2V safety applications;
2. The **Communications Network** – use of DSRC, cellular, or other communications media to transmit encrypted security-related messages between OBEs (and possibly RSEs) and the SCMS; and
3. The **SCMS** – the organizations/functions/infrastructure providing PKI security to the V2V system.

Our interim analysis assumed that any V2V system deployed through a NHTSA regulatory action will have a capability not inherent in the latest SCMS design: the ability for DOT and/or the V2V equipment manufacturers to access information that links problematic certificates/messages collected by the SCMS with production runs or lots of potentially defective V2V equipment. This capability would have ensured that information NHTSA needs for defect and compliance purposes is collected by OEMs and/or relevant SCMS entities and made available to the agency in a timely manner.

As is the case with all such analyses, NHTSA's interim risk assessment included the following procedural steps:

- **Establish Business Needs:** What are the critical business needs that a V2V system must satisfy?
- **Identify System Functions:** What system functions serve those business needs?
- **Identify Data Needs/Transactions:** What data needs/transactions stem from the identified system functions?
- **Describe Nature of Resulting Risks:** What risks result from the collection, storage, or dissemination of data on the system? Do the data transactions increase privacy risks to existing related systems (both safety and security systems within a motor

vehicle, and opt-in systems like OnStar that collect motor vehicle data from on-board systems and transmit it elsewhere)?

- **Identify and Explore Technical/Policy Controls:** As currently envisioned, what technical and policy controls mitigate the identified privacy risks? Should there be others?
- **Determine Likelihood:** What is the likelihood of the risks? Likelihood is calculated for threat, vulnerability, and impact as part of the risk impetus (i.e., an individual or organization's motive for engaging in the activities creating the risk), not the risk itself. This can be expressed as, $L = [(T * V)/I]$. This inquiry necessarily must take into account the relative cost and ease of access to the same data via existing technologies and data sources.
- **Quantify Resulting Risks:** On the basis of consequence/harm and likelihood, what is the impact of the resulting risks, can those risks be mitigated by any controls, and are there risks that remain unmitigated (i.e., residual risk)? Residual risk comes from the application of controls to the risk set $RR = R - I$.
- **Assess Consequences/Harm:** What are the consequences of the potential risks identified?

It is important to emphasize that residual risk stemming from the V2V system will never be zero due the inherent complexity of the V2V system design and the diversity/large number of interacting components/entities, both technological and human. Additionally, technology changes at a rapid pace and may adversely impact system controls designed to help protect privacy in unforeseen ways. For these reasons, as is standard practice in both the public and private sectors, the primary function of a privacy risk assessment is to identify residual risk and its potential consequence/harm. On the basis of that critical information, agency decision-makers then will be in an informed position to determine whether that residual risk is acceptable – and, in the alternative, whether functionality should be sacrificed in order to achieve an acceptable level of residual risk, and if so, what functionality.

On the basis of then available information and stated assumptions, NHTSA's interim risk assessment identified the system's business needs, relevant system functions, nature of the resulting risks, and existing/other technical and policy controls. It also captured the team's attempt to provide an initial rough estimate of the extent, likelihood, and consequences/harm of risk stemming from the system. There was consensus among the team members that, should NHTSA proceed with regulatory action, DOT will need to obtain technical input from external security and privacy experts by proceeding with planned privacy research. Such research will help us to make a more fine-grained estimation of the extent, likelihood, and consequences/harm of risk stemming from the V2V system. It also will assist the Department and NHTSA in garnering public support for V2V by providing technical data to support NHTSA's position that the V2V system protects the privacy of participants and makes geo-locational tracking highly unlikely.

It is important also to note that NHTSA's interim privacy assessment did not take into account the business or informational needs of other DOT modal administrations, other Federal agencies (such as DOJ, DHS, FCC, and FTC), and State and local stakeholders. NHTSA will need to consider whether to expand our assessment to identify and analyze the different or additional privacy risks that may stem from the V2V-related activities and needs of other entities. For example, the safety, mobility, and environmental V2I and V2X applications being developed primarily by FHWA, FMCSA, and their respective stakeholders might generate different or additional information needs. The FTC, as the entity that regulates the privacy relationships between private entities and consumers, may have some interests in the privacy practices and controls (including information collection) designed into V2V security system if the system ends up being owned and managed privately. Finally, the FCC, as regulators of the spectrum, might have informational needs related to their enforcement functions, the collection of which could impact our privacy risk assessment.

1. V2V system needs/functions that necessitate data transactions posing potential risks to privacy

NHTSA's interim privacy analysis identified three categories of V2V system needs/functions that pose potential risks to privacy during data transactions:

- System safety (BSM data sent/received by V2V devices to enable safety applications)
- System security (certificates and other communications between V2V devices and SCMS)
- Agency safety and enforcement functions (data linking V2V device production lots to long-term enrollment certificates)

The critical foundation for NHTSA's privacy risk assessment is the data collected, transmitted, stored and disclosed within, by, and between the V2V system components and other entities. The team identified several data needs/transactions that could introduce privacy risks into the V2V system, including:

- The collection, transmittal, storage, and potential uses of unencrypted GPS and related path history information used in safety applications;
- The collection of data linking long-term security credentials with production runs/lots of V2V equipment used by NHTSA in investigation and recall purposes;
- The certificate and related linkage/bundling data collected and transmitted within the various functions of the SCMS used for distributing certificates; and
- The transmission and storage of location information broadcast when cellular (a potential communication option) is used as a method of communication between V2V devices and the SCMS for security-related purposes used for distributing certificates and other security-related communications.

2. Potential risks to privacy introduced by V2V communications or other data transactions necessary to satisfy system need

The team identified the following potential risks to privacy in the V2V system on the basis of the V2V data transactions that are necessary to satisfy system needs: (a) location tracking via BSM; and (2) identification of individuals and individual behaviors.

a) Location tracking via BSM

NHTSA is aware of concerns that the V2V system could broadcast or store BSM data (such as GPS or path history) that, if captured by a third party, might facilitate very-localized vehicle tracking. In fact, the broadcast of unencrypted GPS, path history, and other data characteristics in or derived from the BSM appears to introduce only very limited potential risks to individual privacy. Preliminary research performed for NHTSA suggests that tracking a specific car or driver based on BSM would be both difficult and costly. Nevertheless, the likelihood of tracking – or availability of information and technologies that facilitate linking location or other BSM data to a specific motor vehicle, address, or person – will be a key inquiry for DOT/NHTSA and their privacy and security consultants going forward.

Research Need VIII-1 V2V Location Tracking via BSM

Research Activity:	Privacy Risk Assessment of V2V System
Description:	Assess the availability of information and technologies that facilitate linking data in the BSM to determine a motor vehicle's path
Target Completion:	2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:
NHTSA will conduct a privacy risk assessment of the V2V system that includes an analysis of the ability of vehicles to be tracked via BSM transmissions and the resultant impact of possible tracking to an individual's privacy

It is theoretically possible that a third party could try to capture the transitory locational data in order to track a specific vehicle. However, we do not see a scenario in which one wishing to track a vehicle would choose the V2V system as the means. Nevertheless, NHTSA is conducting further research to accurately assess the level of privacy risk inherent in the broadcast of unencrypted BSM data.

Other methods exist for tracking a vehicle's location path, such as through electronic emanations from the car itself or from on-board electronics such as cell phones (although DOT consultants advise that both methods are expensive and difficult) and use of a single identifier broadcast from the vehicle (e.g., E-ZPass, OnStar$^{\text{TM}}$). NHTSA's planned comprehensive privacy risk assessment will need to consider the ease and cost of other methods of location tracking in connection with assessing the likelihood of location tracking via data in the unencrypted BSM.

b) Identification of individuals and individual behaviors:

Because a BSM does not identify a specific vehicle or individual, the V2V system as currently designed would not provide such a clear link to a driver or owner. However, the ease with which BSM data characteristics may be used to identify, either directly or indirectly, a specific vehicle, driver, or owner will be a subject of ongoing research and will be central to NHTSA's assessment of the likelihood of various risks to privacy.

Research Need VIII-2 V2V Identification Capabilities

Research Activity: Technical Analysis of the Potential Privacy Risk of V2V Systems

Description: Understanding and quantifying risk of linking vehicle tracking or other information in the BSM to a specific vehicle, address, or individual via available resources (including but not limited to database matching or data mining)

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will conduct a privacy risk analysis of the V2V system that includes an investigation of the use of BSM records to identify a vehicle, address, or individual.

At the component level, the specific potential tracking risks include:

- **OBE/BSM**: Location tracking via radio identification
- **Network Communications**: Location tracking via cellular IP address or computer-specific Wi-Fi address
- **SCMS**: Location tracking via after-the-fact reconstruction of GPS info in linked security certificates

3. Technical, physical and/or policy controls evaluated to minimize potential privacy risks

Generally, privacy risk controls fall into 3 categories:

- **Physical Controls**: Physical protections that reduce privacy risks (for example, a tamper-proof casing around the computer module storing a motor vehicle's certificates or high-security access procedures to gain physical access to an SCMS server facility)
- **Technical Controls**: Data-protective technologies designed into a system
- **Policy Controls**: Laws or organizational policies that make unauthorized data collection, storage, or disclosure less likely by creating organizational and/or functional separation and imposing organizational or legal consequences against hackers or malfeasant insiders

The current V2V security design contemplates a PKI security system that makes use of both asymmetric and symmetric keys and other technical, organizational, and policy controls (including, as applicable, compliance with the Privacy Act, FISMA[223] and other Federal statutes, regulations and policy relevant to privacy in Federal information technology systems) intended to prevent or make far more difficult tracking of devices, either contemporaneously or after the fact. Examples of technical controls in the current security design intended to minimize the risk of tracking via linking of security credential information in the unencrypted BSM include 5 minute certificates and shuffling of certificates prior to reuse.

The SCMS design also anticipates policy controls like organizational and/or functional separation, and organizational consequences to deter collusion that might enable tracking, such as separation of the enrollment function from the certificate issuance/distribution functions; separation of the certificate issuance and distribution functions; and having several certificate shuffling and location-obscuring functions.

As discussed above in connection with governance, ultimately, the SCMS Manager will be the entity that establishes and enforces physical, policy, and technical controls that are applicable to: (1) all of the CME entities that make up the SCMS, and (2) the communications media used by CME organizations to communicate with both V2V devices and RSE. Once greater clarity of the SCMS structure and governance emerges, we will need to inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy risk assessment.

Research Need VIII-3 V2V Inventory of Privacy Controls

Research Activity: Technical Analysis of the Potential Privacy Risks of V2V Systems
Description: Inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy assessment
Target Completion: 2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:
NHTSA will conduct a privacy risk analysis of the V2V system (Research Need VIII-4) that includes the development of an inventory and assessment of privacy controls.

4. Significance of the identified potential privacy risks

Assessing the significance of the potential risks to privacy that stem from the V2V system, in light of identified controls to mitigate those risks, is the final step in a comprehensive privacy analysis. With the help of subject-matter experts, NHTSA will need to quantify the level

[223] Federal Information Security Management Act of 2002.

of each potential privacy risk. The level of privacy risk (typically categorized as high, medium, and low) is a function of:

a) Adverse impacts to privacy that would arise if the circumstance or event occurs; and

b) Likelihood of Occurrence (which necessarily must take into account the relative cost and ease of access to the same data via existing technologies and data sources).

Thus, Privacy Risk = Impact x Likelihood.

Overall, based on present information and our interim privacy assessment, we have reason to believe that a properly-designed V2V system would curtail any serious risks to privacy. The agency acknowledges there may be no way to *entirely* eliminate privacy risks from the V2V system, but believes the efforts expended to develop robust security system designs to protect individual privacy collaboratively through our cooperative research efforts appear to meet that need. However, NHTSA intends to perform an even more comprehensive and definitive assessment of any proposed regulatory action to identify potential risks to privacy and ensure that appropriate controls are in place to help mitigate such risks.

Research Need VIII-4 V2V Privacy Risk Assessment[224]

Research Activity: Technical Analysis of the Potential Privacy Risk of V2V Systems

Description: A comprehensive privacy risk analysis of all aspects of the V2V system including infrastructure equipment, on-board vehicle systems, wireless and wired communications, as well as organizational and management issues. This assessment will include previously identified Research Needs in this section: V2V Location Tracking via BSM; VIII-2, V2V Identification Capabilities; and VIII-3, V2V Inventory of Privacy Controls

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

This privacy risk analysis will provide the information about the latest security design and related privacy risk to enable the Department to perform a comprehensive Privacy Impact Assessment as required by law to determine how to balance individual privacy, data security, and safety.

[224] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

IX. V2V Communications Security

A. Overview and importance of security

Public acceptance and the adoption of cooperative V2V safety applications will depend on appropriate levels of security as an integral part of the system. In contrast to other types of safety technologies, the V2V safety applications are cooperative—meaning that both vehicles must send, receive, and analyze data in real-time. This cooperative exchange of data about potential threats and hazards forms the basis of alerts and warnings to drivers to support their decisions and actions to avert impending incidents. This is a new paradigm that is in contrast to the stand-alone sensor-based vehicle system. However, a cooperative system can only work when participants in the system are able to trust the alerts and warnings issued by V2V devices working with messages from other V2V devices.

Thus, the basis of a relevant V2V security system is "trust"—a requirement that thousands of data messages will be authenticated, in real-time, as coming from a trusted (if unknown) source. It is also a critical element in achieving interoperability—o that vehicles of different make/model/year will be able to exchange trusted data without pre-existing agreements or altering the actual vehicle designs.

Further, the system must be secure against internal and external threats or attacks. Three primary elements of the V2V system require security:

1. Communications (the medium, the messages/data, the certificates, and any other element that supports message exchange);
2. Devices; and
3. Structure (organizational, operational, and physical).

Last, in addition to these requirements, the system needs to be: scalable to meet the needs of over 350 million users across the Nation; extendable to accommodate other types of applications such as V2I mobility, management, and environmental applications; and financially sustainable.

Eleven years of research (i.e., examination of different security approaches, technical architecture and configuration decisions, testing of prototypes, and development of an operational and organizational structure) have resulted in the current security design concept for a V2V system, as discussed below.

Cryptography is the approach that has been used historically to secure communications. Intended recipients have a "key" that allows them to decrypt and read the original message. It can be implemented in varying ways to achieve different levels of security. These include: (a) data confidentiality; (b) data integrity; (c) authentication; (d) non-repudiation (which means a sender cannot deny a message that they have sent); or (e) authorization (grants access rights to others to perform actions).[225]

Encryption techniques rely upon algorithms that have evolved significantly over time and were recently accelerated by the advent of powerful computers. Algorithms are calculations with well-defined steps that can be followed as a procedure—in this case, a procedure to encrypt and decrypt information.

The operations are dependent upon a separate piece of information known as a "key" which can be varied and which then varies the output of the algorithm. In a "symmetric" encryption system, there is one key—the secret key used to encrypt the message is the same one used to decrypt a message. In an asymmetric encryption system, keys come in pairs—each message sent contains one half of this key pair, and the receiving device has the other key.

Advancements in computing power provide industry with the ability to employ advanced algorithms and larger keys, thus making decryption thousands of times more difficult without the key.

1. Security options considered

In considering which option would most effectively provide trusted message exchange and secure communications for safety-critical applications, the DOT and V2V research development team (including CAMP security experts) compared three options—symmetric encryption systems, group signature systems, and asymmetric public key infrastructure systems. When assessing these alternatives, the V2V research team (both DOT and CAMP members) was looking for an option that:

- Did not require the identity of the participating parties and, accordingly, supported the goal of appropriately preserving privacy;
- Was fast enough to fit within the bandwidth constraints of DSRC and the processing constraints of the V2V on-board equipment;
- Entailed a number of over-the-air bytes needed for security that fit within the constraints of DSRC bandwidth and size of the BSM in the message payload; and
- Supported non-repudiation.

[225] Handbook of Applied Cryptography (Menezes, van Oorschot, and Vanstone, ISBN 0-8493-8523-7) at http://cacr.uwaterloo.ca/hac/about/chap1.pdf (last accessed June 28, 2013).

Table IX-1 provides a comparison of the “options” as alternatives and notes that characteristics of each approach are beneficial to the V2V needs or contain “fatal flaws.” The (*) denotes characteristics that do not meet key criteria for the V2V system (safety, security, privacy, latency, cost, non-repudiation are the key criteria) while the (^^) denotes beneficial characteristics.

Table IX-1 Security Approach Alternatives[226,227]

<table>
<tr><td colspan="3">1. <b>Symmetric Key Systems</b>
This approach requires that both parties have the same secret key. Securely distributing keys in such a system becomes infeasible when securing multiple types of devices with a large and expanding base of users. The approach is suitable for systems where the endpoints can be tightly controlled – for example, tolling, or ATMs, or military radio. Asymmetric cryptography is suitable for systems where membership is highly dynamic or where endpoints cannot be so tightly controlled – for example, web browsers or postage stamps.</td></tr>
<tr><th>Cryptography method</th><th>Beneficial Characteristics</th><th>Limitations</th></tr>
<tr><td>Symmetric-key ciphers (stream ciphers, block ciphers)*</td><td>▪ Extremely fast</td><td>Key distribution or pre-storage is:
▪ A security vulnerability and
▪ Too cumbersome at large scale*
▪ There is no non-repudiation.
o Global symmetric-key is more vulnerable to compromise.
o V2V needs authentication for trust, not encryption (BSM not encrypted).</td></tr>
<tr><td>Arbitrary length hash</td><td>▪ Fast, could be used if anchored by periodic certificates</td><td>▪ Need for key distribution in later packets <b>adds over-the -air overhead and slows</b></td></tr>
</table>

[226] Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build computer security systems. These routines include, but are not limited to, one-way hash functions and encryption functions. When creating cryptographic systems, designers use cryptographic primitives as the ir most basic building blocks. Because of this, cryptographic primitives are designed to do one very specific task in a highly reliable fashion. They include encryption schemes, hash functions and digital signatures schemes. Since cryptographic primitives are used as building blocks, they must be very reliable, i.e., perform according to the ir specification. Id.

[227] E.g., Understanding PKI: concepts, standards, and deployment considerations, at 11-15 (Adams & Lloyd, 2003) at Docket No. NHTSA-2014-0022; Managing information systems security and privacy, at 69 (Trček, 2006) at Docket No. NHTSA-2014-0022; Public key infrastructure: building trusted applications and Web services, at 8 (Vacca, 2004) at Docket No. NHTSA-2014-0022; and Network Security with OpenSSL, at 61-62 (Viega, et al., 2002) at Docket No. NHTSA-2014-0022.

functions (MACs)[228], ("keyed hash")		**latency** ▪ May require **precise timing regime** (e.g., TESLA)
Pseudorandom sequences	• Building block for authentication/encryption	• Cannot be used on their own for authentication or encryption
Identification primitives*	▪ Extremely fast	▪ Same key distribution issues as symmetric-key ciphers* ▪ Risk to privacy*

2. Public Key Infrastructure Systems (Asymmetric Key Systems)

Organizations today predominantly use PKI as a primary means of securing communications. This approach allows users to "…securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures." The system also allows for the "…creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. A PKI system creates and manages digital certificates, which maps public keys to entities or permissions, securely stores these certificates in a central repository; distributes them to users as needed (or upon request); and revokes them in the case of misuse, system or devices failures, or malicious behavior." The public key(s) in an entity's certificate can be used to authenticate the entity, directly encrypt data for the entity, or establish a shared symmetric key that can be used to protect bulk data.

Cryptography method	**Beneficial Characteristics**	**Limitations**
Public-key ciphers	▪ Easy distribution of public key ▪ Can distribute pairwise or group symmetric keys for bulk encryption	V2V needs authentication for trust, not encryption (BSM not encrypted).
Signatures	▪ Easy distribution of public key^^ ▪ May gain sufficient speed coupled with appropriate certificate exchange mechanism (e.g., Verify on Demand or Periodic broadcast)	▪ Slower than symmetric systems ▪ Adds more packet overhead than symmetric systems
Identification primitives	▪ Building block for signatures	▪ In general interactive – cannot be used to authenticate broadcast messages.

3. Group Signatures (Subset of PKI Systems)

This approach allows a single public key to verify signatures created by the many unique private keys of all the group members. The keys are issued by a central authority that can identify misbehavers and revoke credentials. Only group members have a valid signature and a member of a group can anonymously sign a message on behalf of the group. The signer is anonymous, except the signer can be identified with the group manager's secret key; thus, the anonymity can be broken by the group manager.

[228] The acronym MAC has two accepted industry definitions depending on the industry and context. For this context it is defined as Message Authentication Code.

Cryptography method	Beneficial Characteristics	Limitations
Group Signatures	▪ Easier key distribution - Single public key verifies many unique private key ▪ Anonymous except to the central authority	▪ Signature too big for over-the -air requirements* ▪ Revocation checking is computationally expensive ▪ Lose backwards privacy protection at revocation* ▪ Master key holder can forge messages and compromise privacy

4. Non-Keyed Systems

These are simply algorithms that are useful building blocks in other cryptographic systems. Note that with the evolution of cryptographic technologies over the years, non-keyed options are no longer considered separate alternatives, but building blocks used to implement either the Symmetric-key or Public-key options. Thus, the first two options are the only actual alternatives to choose from (group signatures were dismissed because of the privacy requirements).

Cryptography method	Beneficial Characteristics	Limitations
Arbitrary length hash functions	Used as building block in keyed methods (e.g., signatures)	Not keyed, so can't be used on their own to establish identity or to encrypt data*
One way permutations	Used as building block for signatures	Not keyed, so can't be used on their own to establish identity or to encrypt data*
Random sequences	Used as building block in keyed methods (e.g., group linkage values). Allow efficient construction of sequences for which an adversary cannot guess the next or previous entry	Not keyed, so can't be used on their own to establish identity or to encrypt data*
Arbitrary length hash functions	Used as building block in keyed methods (e.g., signatures)	Not keyed, so can't be used on their own to establish identity or to encrypt data*

In viewing the tables above, the public key infrastructure option (asymmetric key) using the signature method was deemed to offer the most effective approach to implementing communications security and trusted messaging for a very large set of users. Thus, it was chosen for the BSM. Importantly, the effectiveness of this approach is highly dependent upon the technical design decisions regarding *how* to implement this approach in its given environment.

2. Overview of PKI and how it works

How a PKI architecture is implemented can vary from one system to another. The choices made in configuring a PKI architecture speak to the type of goals and objectives for a system and focus on choices that:

- Support a particular level of strength of security or privacy that is desired or needed by the system, and assure longevity to the security that is longer than the lifespan of the equipped vehicles.
- Support scalability; extensibility to other uses (if desired); system operations, maintenance, upgrades, and evolution needs; and ease of access and use requirements
- Address issues such as technology limitations or constraints, or cost limitations
- Mitigate risks and types of attacks envisioned on the system.

Noting the system objectives articulated by the research team (trusted messaging, feasible operations, and appropriate privacy protection), the following discusses the basic elements of any PKI, and notes the challenge in designing a security approach specific to the V2V system.

All basic PKI systems are comprised of the following elements and functions, at a minimum[229]

- **A Certificate Authority (CA)**—an entity that acts as the "trusted third party" to provide the action to "authenticate" the entities within a network. It typically does so by signing and distributing digital certificates. The CA also typically revokes certificates and publishes a certificate revocation list so that valid users know to ignore certificates of users who have been revoked. A CA is considered the root of trust in a PKI.
- **A Registration Authority (RA)** — the entity that is certified to register users and issue certificates. This function is performed by the CA in the simplest PKI systems.
  - **A Root Certificate Authority** (sometimes the CA and sometimes a separate entity)—the highest trusted entity within a PKI security system, the Root CA typically has a self-signed and issued certificate. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has

[229] E.g., http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx (last accessed Jan. 30, 2014); https://www.juniper.net/techpubs/en_US/junos10.4/information-products/topic-collections/nce/pki-conf-trouble/index.html?topic-49285.html (last accessed Jan. 30, 2014) and www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=8&cad=rja&ved=0CFAQFjAH&url=http%3A%2F%2Facs.lbl.gov%2F~mrt%2Ftalks%2FsecPrimer.ppt&ei=ua7IUdyTBvKv4APlqYCABg&usg=AFQjCNHO-XXndSLpKwls7VHbNsk_Ckmamw&sig2=d5L8IFMnEegw39L1dE-hJA (last accessed Jan. 30, 2014).

  been established, it can be used to authorize subordinate CAs to issue certificates on its behalf.[230]

  - **Digital Certificates** (also known as public key certificates)—electronic "documents" that use a digital signature to bind a public key with an identity.[231] Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root CA. Many software applications assume these root certificates are trustworthy on the user's behalf. For example, a web browser uses them to verify identities within SSL and TLS secure connections. However, this implies that the user trusts their browser's publisher, the certificate authorities it trusts, and any intermediates the certificate authority may have issued a certificate-issuing-certificate, to faithfully verify the identity and intentions of all parties that own the certificates. This (transitive) trust in a root certificate is the usual case. The most common commercial variety is based on the International Telecommunication Union Telecommunication Standardization Sector standard X.509.[232]
- **Secure hardware and software** (servers, stores, repositories; also known as a central directory)—hardware and software to support the processing of certificate requests, save issued certificates before they are distributed, or save revoked certificates. May generate certificates and validate received certificates. Also used in back-up systems.
- **Communications**—wire line, wireless, or Internet services that provide the communications capacity over which management capabilities are enacted to receive requests, distribute certificates, collect misbehavior reports, revoke certificates, and distribute the CRL. Average sizes of PKI objects are:
  - Private/public key pair = typically 1 KB
  - Local certificate = 2 KB
  - CA certificate = 2 KB
  - CA authority configuration = 500 bytes
  - CRL (average size is variable, depending on how many certificates have been revoked by a particular CA) = typically between 300 bytes to 2MB+

Basic technologies used in achieving security levels with these PKI elements include the following.[233]

- Encryption provides confidentiality; can provide authentication and integrity protection
- Hash algorithms/checksums provide integrity protection; can provide authentication
- Digital signatures provide authentication, integrity protection, and non-repudiation.

[230] See http://technet.microsoft.com/en-us/library/cc778623(v=ws.10).aspx (last accessed Feb. 25, 2014).

[231] See www.verisign.com.au/repository/tutorial/digital/intro1.shtml (last accessed Jan. 30, 2014).

[232] See www.itu.int/rec/T-REC-X.509 (last accessed Jan. 30, 2014).

[233] An Introduction to Distributed Security Concepts and Public Key Infrastructure (PKI) (Mary Thompson) See www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=8&cad=rja&ved=0CFAQFjAH&url=http%3A%2F%2Facs.lbl.gov%2F~mrt%2Ftalks%2FsecPrimer.ppt&ei=ua7IUdyTBvKv4APlqYCABg&usg=AFQjCNHO-XXndSLpKwls7VHbNsk_Ckmamw&sig2=d5L8IFMnEegw39L1dE-hJA (last accessed Jan. 30, 2014).

All of these approaches are employed in the V2V security design concept, as well as some unique technologies such as butterfly keys and linkage values that will be defined in the next section.

3. Limitations of existing PKI systems

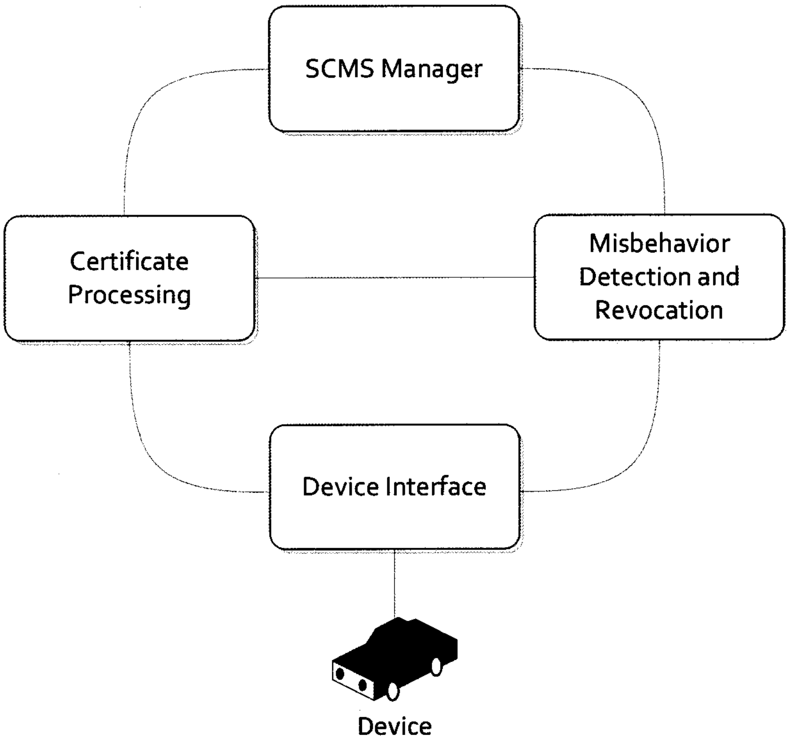
No other PKI system exists today that is broad enough to serve as a key safety-critical model. Most other systems involve data exchange among parties that are either known to each other as trusted sources (e.g., the military knows each of its communication points) or are identifiable (e.g., the FAA air traffic controllers around the Nation can identify each of the planes involved in safety-critical data exchange). Also, most other safety-critical systems employ highly secure networks (e.g., the military) or private networks (e.g., the military) and cannot leverage either existing communications systems or the Internet (to keep capital investment costs to a minimum and to achieve widespread access) in a manner that does not introduce additional vulnerabilities and risks.

Most of the existing commercial systems, by comparison, do leverage the Internet and wireless systems. These systems enable on-line purchasing or on-line financial transactions in a way that allows for easy accessibility to millions of users. They do not, however, meet the level of privacy protection, as these organizations have pre-existing agreements with the CA and thus user identity resides within databases and is typically used as part of the authentication process.

B. Current V2V security design concept

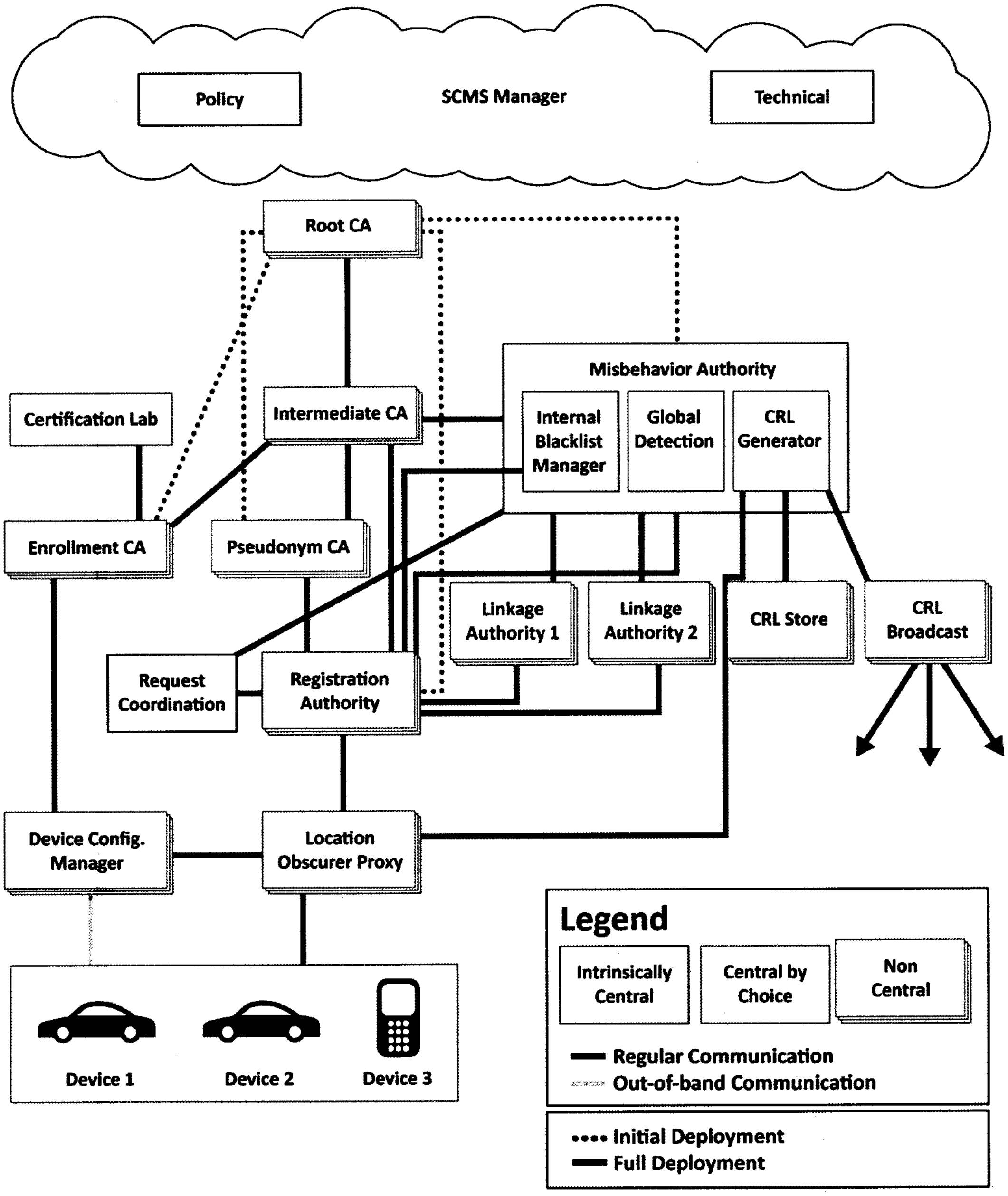
Figure IX-1 presents, at a high level, the basic use-cases of the V2V security system. They are similar to the basic functions of any PKI.

Figure IX-1 Simplified V2V Security System



The remainder of this section expands upon this basic design to present the current V2V security design. Figure IX-2 illustrates the complexity of the V2V security design associated with meeting V2V environment needs. After the illustration, each component is defined.

Figure IX-2 Current V2V Security System Design for Deployment and Operations



This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model where there is no Intermediate CA and the Root CA talks to the MA, PCA, and ECA (dotted lines). In the full deployment model, these entities communicate with the Intermediate CA instead of the Root CA to protect the Root CA from unnecessary exposure (solid line).